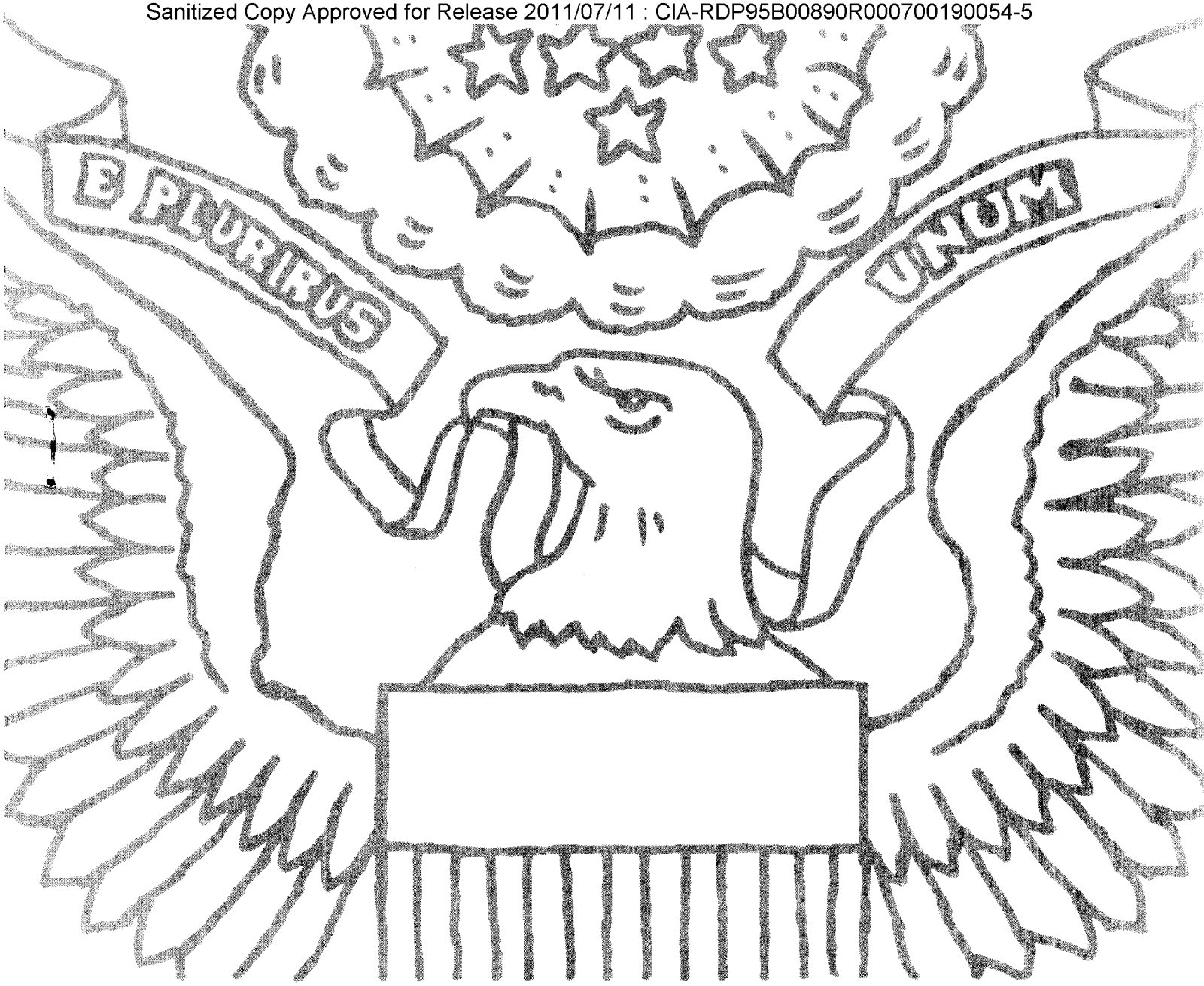
Next 1 Page(s) In Document Denied



Annual Report to the President FY 1982

Information Security Oversight Office

General Services Administration
Information Security Oversight Office
Washington, DC 20405

June 30, 1983

The President
The White House
Washington, DC 20500

Dear Mr. President:

I am pleased to submit the Information Security Oversight Office's (ISOO) 1982 Report to the President.

Established under Executive Order 12065 and continued under Executive Order 12356, effective August 1, 1982, the ISOO oversees the information security program throughout the executive branch. The ISOO is an administrative component of the General Services Administration, but receives its policy direction from the National Security Council.

The 1982 Report contains two sections. The first section comprises a statistical breakdown and analysis of the government-wide information security program. The most recent data cover E.O. 12065's last year of operation, and they generally compare favorably with those of prior years. They demonstrate strong government-wide management of the information security system.

The Appendix to the regular report is an ISOO authored paper entitled, "The Background of Executive Order 12356." It represents an effort to explain to the varied audience of this Report the reasons behind the decision to replace E.O. 12065 with E.O. 12356. The paper is written from ISOO's perspective and, in whole or in part, does not necessarily reflect the views of any other agency.

Because FY 1983 represents the first full year of E.O. 12356's operation, ISOO has been monitoring this critical time period very closely. I will describe the Order's initial successes and problems in ISOO's next report to you.

Respectfully,

Steven Garfinkel

STEVEN GARFINKEL
Director

SUMMARY OF FY 1982 PROGRAM ACTIVITY

Classification Activity

a. At the end of FY 82, 1,465 officials were authorized to classify originally at the "Top Secret" level, 4,073 others at the "Secret" level, and 1,396 others at the "Confidential" level. Since 1972, agencies have reduced the number of original classification authorities from 59,316 to 6,934, an 88 percent reduction.

b. The 17 million original and derivative classification decisions made by agencies in FY 82 are within one percent of the number generated in FY 81. Three percent of the information was "Top Secret," 31 percent "Secret," and 66 percent "Confidential," figures which compare favorably with FY 80 and FY 81.

c. As in previous years, original classification constituted only 6 percent of all classification decisions and derivative 94 percent.

d. Two agencies, the Department of Defense and the Central Intelligence Agency, generated nearly 98 percent of all classified information.

Declassification Activity

a. Agencies experienced a 191 percent increase in the number of mandatory review requests over the number received in FY 80, and a 78 percent increase over FY 81. They processed nearly 60 percent, and of these declassified the information in whole or in part in 86 percent of the cases. Agencies processed 214 percent more requests in FY 82 than in FY 80 and 93 percent more than in FY 81.

b. Agencies also experienced a significant increase in the number of appeals received and processed. They increased the percentage rate of appeals declassified in whole from 15 percent in FY 81 to 40 percent in FY 82.

c. Agencies systematically reviewed nearly 20 million pages for declassification, 78 percent less than the number reviewed in FY 80 and 38 percent less than in FY 81. They declassified 85 percent of the information reviewed as compared to 27 percent in FY 80 and 91 percent in FY 81.

Inspections

Agencies conducted over 28,000 self-inspections, 9 percent less than in each of the previous two years. During the inspections agencies detected over 20,000 violations of the Order, implementing directives and regulations.

"Top Secret" Inventories

Agencies reported a "Top Secret" inventory of 1,434,668 documents at the end of FY 82, a reduction of 18 percent from FY 81.

FY 82 Program Strengths

a. Continuing reduction in the number of original classifiers.

b. Continuing management control to prevent the proliferation of classification actions.

c. Improved processing of mandatory review requests and appeals.

d. Agency emphasis on actions to reduce the "Top Secret" inventory.

FY 82 Program Weaknesses

a. Decreased agency activity in the program for systematically reviewing information for declassification.

b. Decreased agency self-inspection activity and the need for improvement in both the quality and thoroughness of agency inspections.

c. Increase in the number of "Top Secret" actions reported by agencies.

INFORMATION SECURITY OVERSIGHT OFFICE

THE INFORMATION SECURITY PROGRAM

FY 1982

The Information Security Oversight Office (ISOO), established by Executive Order 12065 on December 1, 1978, functions now under Executive Order 12356, signed by President Reagan on April 2, 1982. ISOO is responsible for overseeing the information security programs of all executive branch agencies that create or handle national security information and for reporting annually to the President on the state of the program. ISOO monitors the information security programs of approximately 65 departments, agencies or independent offices in the executive branch that create and/or handle national security information.

ISOO is located administratively in the General Services Administration but receives its policy direction from the National Security Council. The Administrator of General Services appoints the ISOO Director upon approval by the President. The ISOO Director appoints its staff, which numbers between 13-15 persons. ISOO funding is included in the budget of the National Archives and Records Service. For FY 1982, ISOO's budget was $518,000.

To meet its responsibilities, ISOO: (a) conducts on-site inspections or program reviews of monitored agencies; (b) gathers and analyzes statistical data on agency programs; (c) sponsors or produces educational programs or materials on information security; (d) develops and issues implementing directives or instructions regarding the Order; (e) receives and takes action on suggestions, complaints, disputes and appeals from inside or outside the Government on any aspect of the administration of the Order; and (f) conducts special studies of the information security system. This evaluation of the executive branch's information security program for FY 1982 is based upon program reviews and inspections and the compilation and analysis of statistical data regarding program activity.

A. PROGRAM REVIEWS AND INSPECTIONS

To facilitate coordination and continuity of oversight operations, ISOO analysts serve as liaison with specific executive branch agencies. It is their responsibility to stay abreast of relevant activities within assigned agencies, to coordinate with their agency security counterparts on a continuing informal basis, and to conduct formal inspections of assigned agencies in accordance with a planned annual inspection schedule.

These on-site formal inspections concentrate on all aspects of the information security program, including classification, declassification, safeguarding, education and training, administration, and marking. They always include in-depth discussions or interviews with agency security officers, classifiers and handlers of national security information. To the maximum extent possible, ISOO analysts also review a sampling of classified documents to ascertain the proper application of markings; the correct assignment of classification and level of classification in relation to the information's sensitivity; and the degree of compliance with safeguarding requirements. ISOO analysts recommend corrections, either on-the-spot or as part of a

formal inspection report. These formal inspections are a necessary tool for identifying and resolving problem areas since they provide indicators of program compliance or non-compliance that are not apparent or available from statistical data.

B. STATISTICAL REPORTING

Agencies have been required to report statistical data on their programs since the inception of an oversight organization. Over the years changes have been made in the reporting requirements in order to provide more reliable and meaningful data upon which to base program evaluations. Moreover, consistent with efforts to achieve paperwork reductions, the frequency of reporting has been changed from quarterly to annually. During FY 1982, ISOO continued this trend by revising its Standard Form 311, on which agencies report on their activities. For FY 1982, agencies were required to report on the following:

1. The number of original classification authorities;

2. the number of original classification decisions, broken down by classification level and duration of classification;

3. the number of derivative classification decisions;

4. agency decisions on requests and appeals for mandatory review of information for declassification;

5. the number of pages reviewed for declassification on a systematic basis and the number declassified;

6. the number of formal agency inspections;

7. instances of infractions detected during agency inspections;

8. the number of "Top Secret" documents held in inventory; and

9. in narrative format, agency activities related to declassification, training, safeguarding, the use of the balancing test, and program management.

Because Executive Order 12356 became effective on August 1, 1982, agency reports for FY 1982 covered only a 10-month period. ISOO has increased reported figures by 20 percent for those data ordinarily reported on an annual basis. This facilitates comparison with the numbers for prior reporting periods.

C. CLASSIFICATION ACTIVITY

1. Original Classification Authorities (Exhibits 1-5). During FY 1982, executive branch agencies continued to reduce the number of officials authorized to classify national security information originally. This statistic is particularly noteworthy because, in ISOO's experience, the number of original classifiers is one of the most important systemic controls on the quality and quantity of classification decisions. Since FY 1980, the number of "Top Secret" authorities has been reduced by 36 (two percent), "Secret" authorities by 61 (two percent), and "Confidential" authorities by 118 (eight percent). At the end of FY 1982, only 1,465 officials were authorized to classify originally at the "Top Secret" level, 4,073 others at the "Secret" level, and 1,396 others at the "Confidential" level. Since 1972, agencies have reduced the total number of original classification authorities from 59,316 to 6,934, an 88 percent reduction.

Exhibit 1
Original 'Top Secret' Authorities

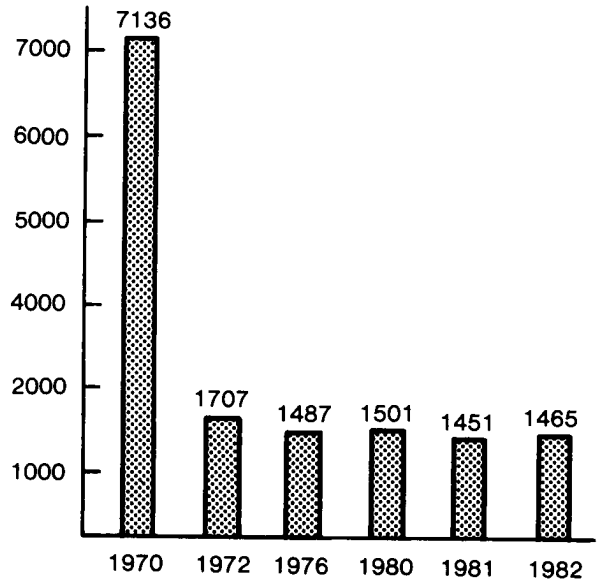


Exhibit 2
Original 'Secret' Authorities

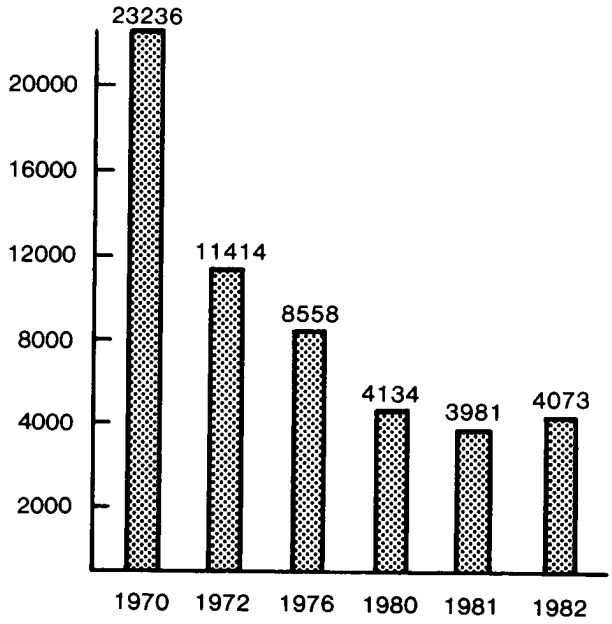


Exhibit 3
Original 'Confidential' Authorities

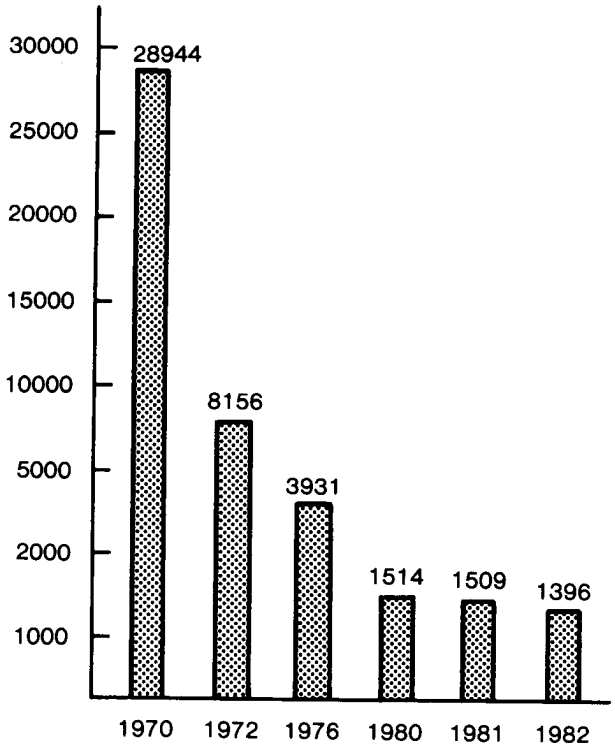


Exhibit 4
Overall Original Authorities

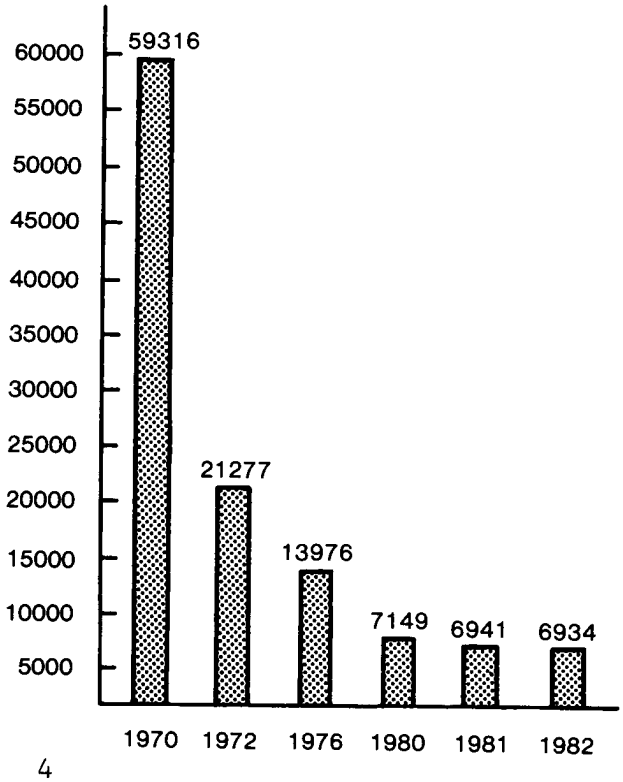


Exhibit 5

The Shrinking Circle of Original Classifiers

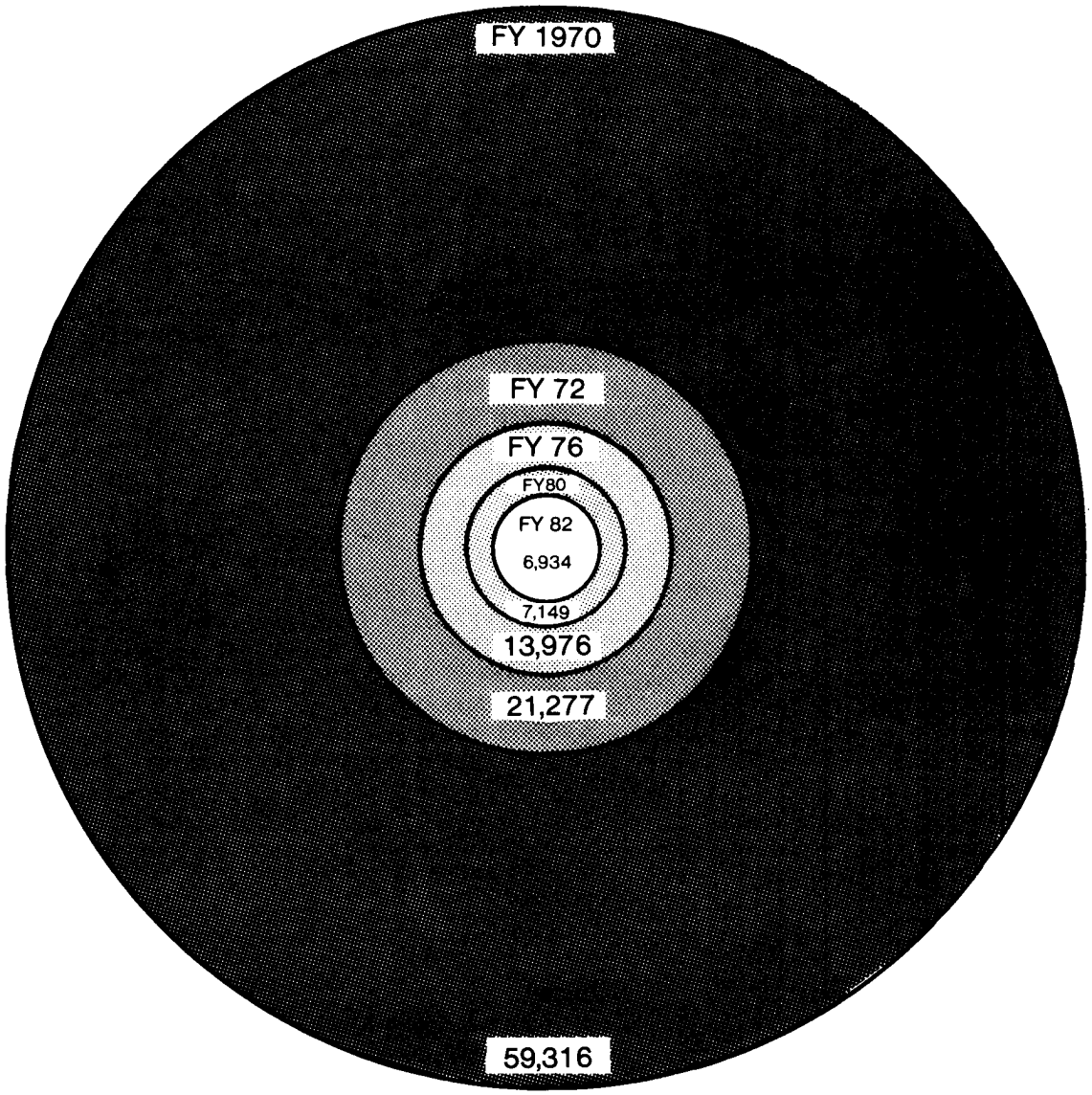
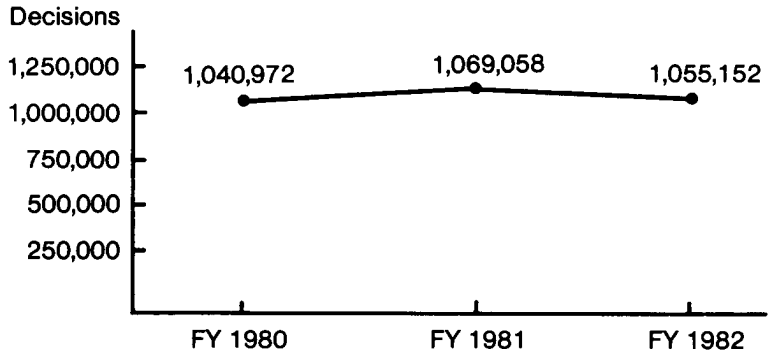


Exhibit 6

Comparison of Original Classification Activity



2. Original Classification Decisions (Exhibits 6-7). For FY 1982, the number of original classification decisions was essentially the same as reported for FY 1980 and FY 1981. They totaled 1,055,152, of which two (2) percent were classified at the "Top Secret" level, forty-one (41) percent at the "Secret" level, and fifty-seven (57) percent at the "Confidential" level. With respect to duration of classification, thirty-four (34) percent were assigned declassification or review dates from one to six years from their creation and sixty-six (66) percent from six to twenty years. These distributions are also in line with those reported for FY 1980 and FY 1981. Comparison reveals one statistic that requires increased oversight; i.e., the significant increase in the number of original "Top Secret" classification decisions. The number reported for FY 1982 exceeds the number reported for FY 1981 by forty-five (45) percent. Consistent with previous years, over ninety-nine (99) percent of all original classification activity was concentrated in four agencies: CIA (39.19%), DOD (27.66%), State (16.84%) and Justice (15.42%). All other agencies of the executive branch accounted for less than 10,000 (.89%) original classification decisions.

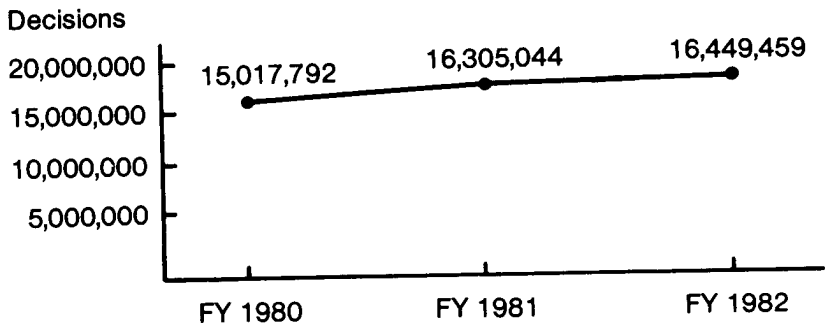
Exhibit 7

FY 1982 Original Classification Activity By Agency

Agency	Original Decisions	%0-6 yrs.	%6-20 yrs.	%TS	%S	%C
CIA	413,521	8%	92%	4%	55%	41%
DOD	291,831	71%	29%	1%	18%	81%
State	177,673	62%	38%	.1%	20%	79.9%
Justice	162,691	.2%	99.8%	1%	70%	29%
NSC	2,999	86%	14%	8%	49%	43%
FEMA	2,266	17%	83%	20%	47%	33%
DOE	918	74%	26%	2%	28%	70%
Treasury	796	96%	4%	.6%	6%	93.4%

Exhibit 8

Comparison of Derivative Classification Activity



3. Derivative Classification Decisions (Exhibits 8-9). Derivative classification is the act of incorporating, paraphrasing, restating or generating in new form information that is already classified, and marking the newly developed material consistent with the markings of the source information. Agencies reported 16,449,459 derivative classification decisions for FY 1982, which represents less than a one (1) percent increase over the total reported for FY 1981. Of the total derivative actions, three (3) percent were classified at the "Top Secret" level, thirty (30) percent at the "Secret" level, and sixty-seven (67) percent at the "Confidential" level. This is essentially the same distribution pattern as reported for FY 1980, but reflects a two (2) percent reduction in the percentage of documents classified derivatively at the "Top Secret" level in FY 1981.

Two agencies accounted for 99.64 percent of all derivative classification: DOD (83.52%) and CIA (16.12%). This is almost identical with the figures for FY 1980 and FY 1981. All other agencies derivatively classified less than 60,000 actions during FY 1982.

Exhibit 9

FY 1982 Derivative Classification Activity By Agency

Agency	Total Derivative Actions	% TS	% S	% C
DOD	13,738,420	3%	21%	76%
CIA	2,651,466	7%	76%	17%
Justice	25,380	3%	96%	1%
DOE	14,492	2%	12%	86%
FEMA	4,369	8%	63%	29%
Treasury	2,268	2%	40%	58%
NSC	1,898	5%	54%	41%
State	298	0%	74%	26%

Exhibit 10
Comparison of Combined Classification Activity

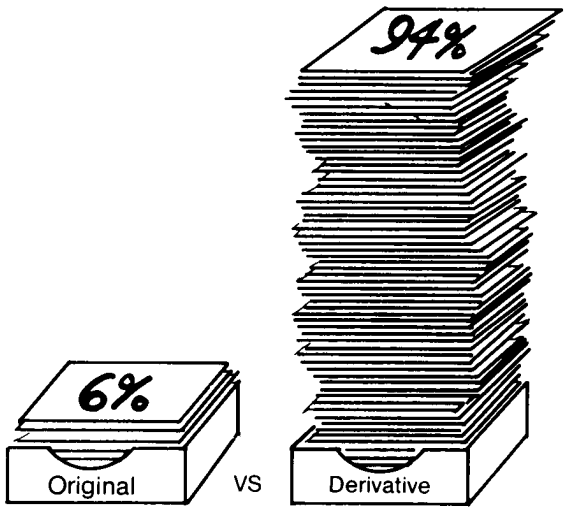
FY	Total Actions	% TS	% S	% C
1980	16,058,764	3%	29%	68%
1981	17,374,102	5%	29%	66%
1982	17,504,611	3%	31%	66%
CHANGE:				
FY 82-81	+130,509 (+.75%)	-2%	+2%	0%
FY 82-80	+1,445,847 (+9%)	0%	+2%	-2%

4. Combined Classification Decisions (Exhibit 10). The total number of original and derivative classification decisions for FY 1982 was 17,504,611, less than a one (1) percent increase over the total for FY 1981. Combined classification assignments placed three (3) percent of all actions in the "Top Secret" category, thirty-one (31) percent in the "Secret" category, and sixty-six (66) percent in the "Confidential" category. The figures compare with those reported during FY 1980 and FY 1981.

The DOD (80.16%) and the CIA (17.5%) accounted for 97.66 percent of all classification activity in FY 1982. All other executive branch activities classified less than 410,000 actions.

5. Original vs. Derivative Classification (Exhibit 11) During FY 1982, the ratio of original to derivative classification decisions remained consistent with the breakdown of recent years; i.e., original constituting six (6) percent of all classification actions and derivative ninety-four (94) percent. Another way of observing this ratio is to

Exhibit 11
Original vs. Derivative



predict that, on the average, each original classification decision will ultimately be reflected in 20 classified documents. This one statistic illustrates the need to concentrate oversight efforts on controlling the quantity and quality of original classification decisions.

D. DECLASSIFICATION ACTIVITY

1. Mandatory Review for Declassification (Exhibits 12 and 13). Executive Order 12065 provided that agencies or members of the public could request that information in an executive branch agency be reviewed for declassification. This prerogative could be exercised at any time during the life of the document. This program has been increasingly popular with members of the public, particularly researchers, since its inception in 1972. Executive branch agencies have acted responsibly in meeting the requirements for mandatory review and have, in whole or in part, provided requesters with approximately eighty-five (85) percent of the information requested. Consistent with the program's popularity, executive branch agencies reported a 191 percent increase in FY 1982 over the new cases received during FY 1980, and a seventy-eight (78) percent increase over cases received in FY 1981. In FY 1982, agencies had a total of 11,871 cases for action. They processed 6,919 (58%) of these cases during FY 1982. Of those processed, 4,500 (65%) were granted in full, 1,446 (21%) were granted in part, and 973 (14%) were denied in full. Agencies processed 4,713 (214%) more cases in FY 1982 than in FY 1980, and 3,334 (93%) more cases than in FY 1981, while maintaining a percentage rate of sixty-five (65) for documents granted in full. Moreover, they reviewed nearly 1,370,000 more pages for declassification in FY 1982 than in FY 1980, and 1,290,000 more than in FY 1981. This represents a twelve-fold increase in agency workload. At the end of FY 1982, forty-two (42) percent of the cases received by the agencies had not been processed and were carried over to FY 1983.

Exhibit 12

Mandatory Review Requests Received

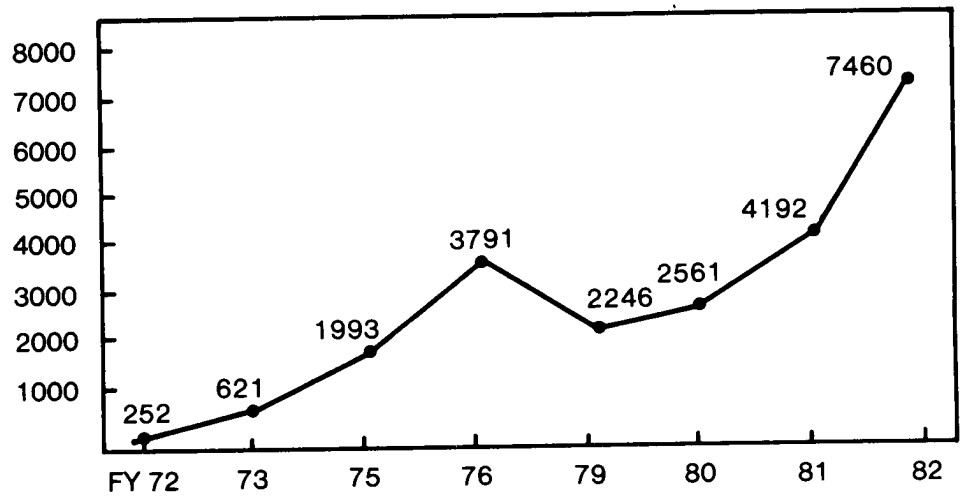


Exhibit 13

FY 1982 Mandatory Review Actions By Agency

Agency	Total Cases Acted On	% Granted In Full	% Granted In Part	% Denied In Full
DOD	3886	77%	8%	15%
State	1077	52%	34%	14%
NSC	820	48%	48%	4%
Justice	576	52%	26%	22%
CIA	190	28%	49%	23%
NASA	113	34%	66%	0%
GSA/NARS	92	45%	35%	20%

2. Mandatory Review Appeals (Exhibit 14). Executive Order 12065 provided that agencies or members of the public could appeal denials from requests for declassification of national security information. As in the case of mandatory review requests, executive branch agencies experienced a significant increase in the number of appeals received in both FY 1981 and FY 1982, as compared with the number in FY 1980. In FY 1982, agencies had a total of 1,451 unprocessed appeals, including carryovers from 1981, and acted on 548 (38%) of them during the year. Of these, 218 (40%) were granted in full, 140 (26%) were granted in part, and 190 (34%) were denied in full. Notwithstanding the additional workload, agencies increased the percentage rate of appeals granted in full from fifteen (15) to forty (40) percent. Seventy (70) percent of all appeals were directed to the Department of Justice, which granted, in whole or part, seventy (70) percent of the appeals it processed.

EXHIBIT 14
Appeals Received

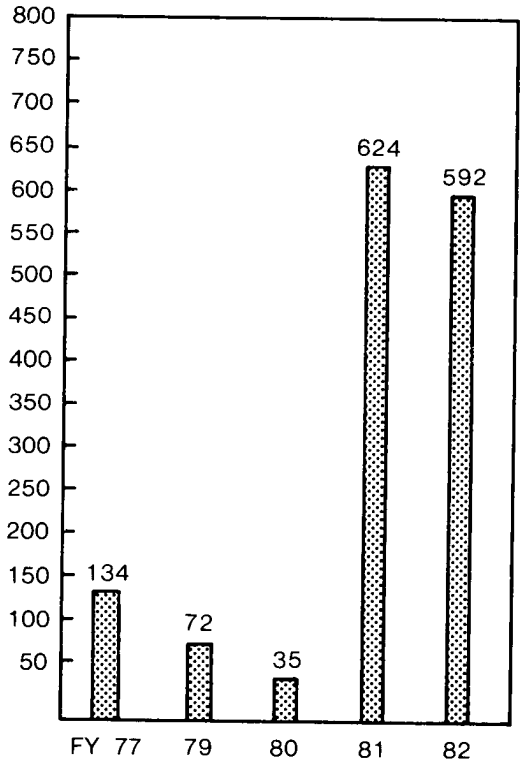


Exhibit 15
Pages Reviewed For Declassification

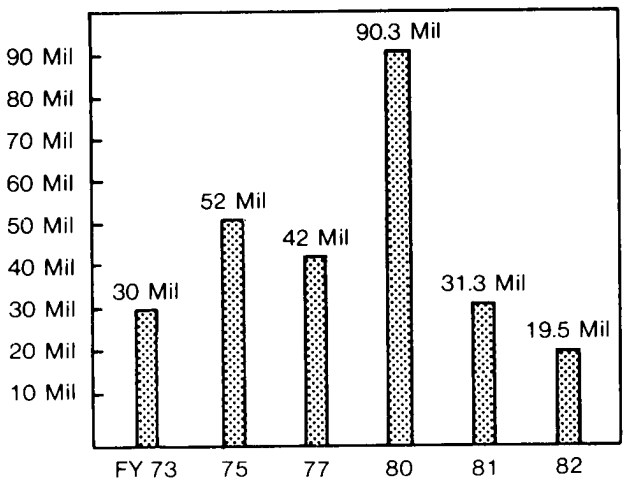
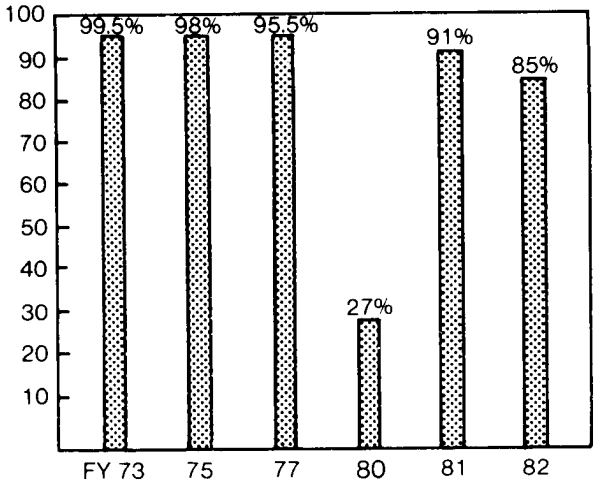


Exhibit 16
% of Reviewed Pages Declassified

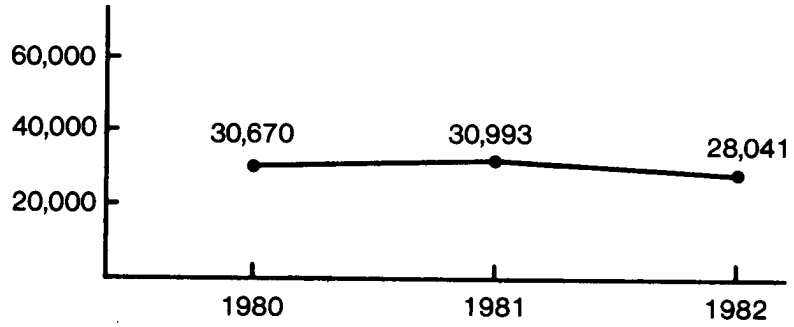


3. Systematic Review for Declassification (Exhibits 15-17). Executive Order 12065 required agencies to review permanently valuable national security information for purposes of declassification as the information became twenty (20) years old. Agencies reported that during FY 1982, they systematically reviewed 19,503,813 pages of national security information. Of these, 16,582,972 pages were declassified. This eighty-five (85) percent declassification rate far exceeded the twenty- seven (27) percent rate achieved in FY 1980, and was just shy of the ninety-one (91) percent rate of FY 1981. The nineteen million pages reviewed for declassification in FY 1982 were, however, seventy-eight (78) percent less than the number of pages reviewed in FY 1980, and thirty-eight (38) percent less than the number reviewed in FY 1981. Most of this reduction can be attributed to the reduction in resources available in the National Archives and Records Service (NARS) for the conduct of systematic review, and a shift of those remaining resources to projects which are especially sensitive and may not be declassified by bulk methods. During FY 1982, there were slightly more than three million pages reviewed in NARS as compared with over eighty-two (82) million pages in FY 1980.

Exhibit 17
FY 1982 Systematic Review Actions By Agency

Agency	Total Pages Reviewed	Pages Declassified	Percent Declassified
DOD	13,815,145	13,268,386	96%
GSA/NARS	3,115,620	2,960,362	95%
CIA	2,153,464	270,610	13%
USIA	216,000	72,000	33%
STATE	102,600	99,522	97%
JUSTICE	50,316	4,260	8%

Exhibit 18
Agency Self-Inspections



E. AGENCY INSPECTIONS

1. Number of Inspections (Exhibit 18). During FY 1982, executive branch agencies conducted 28,041 self-inspections. This represents a nine (9) percent reduction from the number conducted in FY 1980 and FY 1981. Because Executive Order 12065 had been in place for several years and it was common knowledge that efforts were under way to replace the Order, it is not surprising that the number of agency self-inspections declined in FY 1982. With a new Order in place, the number of agency self-inspections should increase significantly in FY 1983.

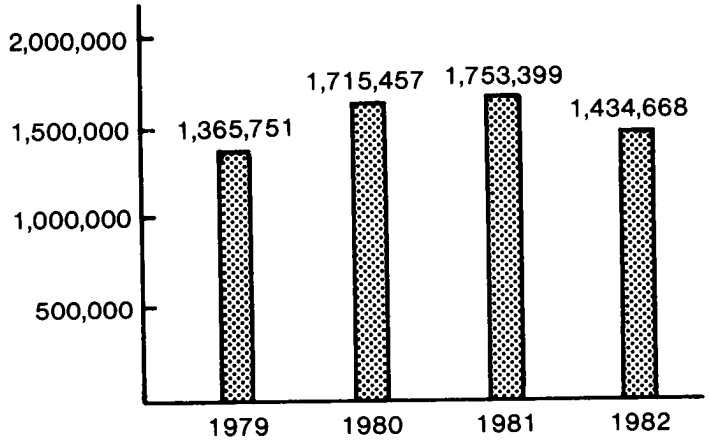
2. Infractions (Exhibit 19). Infractions are minor violations of the Order, its implementing directives or regulations. They do not include those more serious violations that are to be reported to the ISOO Director when they are discovered. For FY 1982, agencies detected 20,279 infractions in their information security program during self-inspections. This number represents an increase over the number of infractions reported for FY 1980 and FY 1981 (some categories of infractions were not included in prior reports). The detection rate of less than one infraction per agency self-inspection for FY 1982 is far less than that experienced by ISOO during its inspections. This statistic calls for greater attention to the quality of agency self-inspections by both ISOO and the agencies.

Exhibit 19
Infractions Detected by Agencies During Self-Inspections

Infraction	#Detected FY 1980	#Detected FY 1981	#Detected FY 1982	% Change From FY 80	% Change From FY 81
Unauthorized Access	950	476	475	-50%	0%
Mismarking	11,297	8,797	11,499	+2%	+31%
Unauthorized Transmission	1,282	924	1,197	-7%	+29%
Improper Storage	3,975	3,341	4,222	+6%	+26%
Unauthorized Reproduction	300	135	207	-31%	+50%
Overclassification	NOT REPORTED		290		
Underclassification	NOT REPORTED		365		
Misapplication of Time Limits	NOT REPORTED		897		
Classification w/o Authority	NOT REPORTED		392		
Extension of Classification w/o Authority	NOT REPORTED		70		
Improper Method of Destruction	NOT REPORTED		665		

F. "TOP SECRET" INVENTORIES (Exhibit 20). Executive branch agencies reported that there were 1,434,668 "Top Secret" documents being held in inventory at the end of FY 1982. This figure indicates that the agencies made significant progress in reducing the more sensitive and costly "Top Secret" inventory by eighteen (18) percent from the total reported in FY 1981.

EXHIBIT 20
'Top Secret' Inventory



Sanitized Copy Approved for Release 2011/07/11 : CIA-RDP95B00890R000700190054-5

APPENDIX

THE BACKGROUND OF EXECUTIVE ORDER 12356

INTRODUCTION

On December 1, 1978, Executive Order 12065, "National Security Information," took effect. Less than four years later, Executive Order 12356 replaced it. What hastened the change? The Information Security Oversight Office (ISOO), charged with overseeing the government-wide information security program under both Executive orders, concludes that the authors of E.O. 12065, in an effort to emphasize the principle of open access to information, included language that sometimes undermined its effectiveness as an information security system.

This is not to say that E.O. 12065 was a failure. As this Report and ISOO's prior Reports to the President illuminate, the Government's information security program was reasonably successful under E.O. 12065. Many of its provisions, most notably those that limited the number of original classifiers and those that required effective training and oversight, have had a very positive impact on the information security program, and are retained or even strengthened in E.O. 12356. As a matter of fact, E.O. 12356 more closely resembles E.O. 12065 than it does any prior information security system.

Retaining its predecessor's successful features, E.O. 12356 abandons or adjusts those aspects of E.O. 12065 that proved to be inefficient, inflexible or counterproductive. Without describing each and every change, ISOO groups the shortcomings of E.O. 12065 into the following categories: (a) its inefficient program for the systematic declassification review of information; (b) its inflexible administrative requirements; (c) its negative tone; (d) its adverse impact on litigation; and (e) its unrealistic program for automatic declassification. In the discussion that follows, ISOO examines each of these problem areas in greater detail, and notes the changes in E.O. 12356 designed to remedy them. They are discussed in the order that each problem arose as a matter to be addressed in the process of constructing E.O. 12356.

THE SYSTEMATIC REVIEW PROGRAM

In 1972, Executive Order 11652 introduced the program of systematic review for declassification. It was designed to promote the expeditious, inexpensive and wholesale declassification of the massive volume of permanently valuable classified records in the National Archives of the United States that dated from World War II and its aftermath. The Order provided that the Archivist of the United States would conduct a systematic review of the Archives' classified holdings as they became 30 years old.

The systematic review program under E.O. 11652 was a tremendous success. Between 1972 and 1978, the National Archives declassified over 100 million

pages of previously classified records. In retrospect, much of the success of the systematic review program at that time was due to the nature of the records being reviewed, most of which related to military operations or emergency planning, and the high priority given the program in the National Archives. Looking at the success of the systematic review program, the drafters of E.O. 12065 decided to take it a few steps farther. E.O. 12065 directed all agencies, not just the National Archives, to conduct a systematic review program, and lowered the applicable age of records to be reviewed from 30 to 20 years. Agencies were further directed to reduce their backlog of permanently valuable classified records in order to complete the transition to 20-year review no later than December 1, 1988.

From its earliest stages of implementation, the revised system faced obstacles, especially in those large classifying agencies that had never conducted their own systematic review programs. They had to divert money from mission related programs to fund new systematic review units. Frequently, the personnel in these units were performing a function that was both new to them and largely unrelated to their previous experience.

The shift to 20-year review created even greater problems. Several factors came into play that sharply reduced the percentage of records that could be declassified as a result of systematic review. First, the general subject areas of the post-War records related more to "Cold War" issues than to military operations and emergency planning. Much more information, frequently involving intelligence activities, remained sensitive. This required item-by-item review, rather than the bulk declassification that spurred the program under E.O. 11652. Second, experience revealed that the national security sensitivity of a significant percentage of information lingers after 20 years, but often dissipates around 30 years. Speculation ties this phenomenon to the fact that the 30-year period more accurately reflects the span of political or public careers. It is worth noting that the Federal Records Act contains a 30-year rule for specific agency restrictions on access to records in the National Archives and a number of foreign democracies restrict access to their records for the same time period. Finally, the 10-year reduction vastly increased the volume of information subject to review, exaggerated by the tremendous growth of the Federal Government during and immediately after the War. Rather than absorbing the backlog, most agencies had made little, if any, progress from the 30-year mark by the August 1982 effective date of E.O. 12356.

In June 1980, the General Accounting Office (GAO), working at the behest of the House Subcommittee on Government Information and Individual Rights, asked ISOO and several other executive branch agencies to review and comment on a draft report entitled, "Systematic Review for Declassification -- Do Benefits Equal Cost?" The draft report answered its title, "No," and went so far as to recommend an amendment to E.O. 12065 to abolish the systematic review program. The draft report stated that agencies could meet researcher demands by relying exclusively upon individual access requests under the Freedom of Information Act or the mandatory review provisions of E.O. 12065.

To coordinate a reply to the draft report, the ISOO Director convened a meeting of the Interagency Information Security Committee, composed of representatives of the major classifying agencies. At the meeting there was almost total

agreement that the GAO draft correctly pointed out a number of deficiencies in E.O. 12065's systematic review program. (The meeting also featured the first formal expression of other problems with E.O. 12065 by several agency representatives.) The representatives took sharp issue, however, with the draft report's recommendation to abolish the program entirely. There was a consensus that Freedom of Information and mandatory review requests could never adequately substitute for the broader scale benefits of systematic review. ISOO, on behalf of the executive branch, strongly objected to GAO's draft recommendation, and stated that it would examine less drastic means of equating the tangible and intangible benefits of the systematic review program with its rising costs. The final GAO report took cognizance of the effort to preserve the systematic review program while lowering the costs; and ISOO's examination of the systematic review program played a major role in the changes that appeared in E.O. 12356.

The systematic review program of E.O. 12356, as implemented by ISOO Directive No. 1, resembles the successful program of E.O. 11652. Once again, only the Archivist of the United States is required to conduct a systematic review program for the declassification of records accessioned into the National Archives, and of presidential papers or records under the Archivist's control. The Directive schedules systematic review at the 30-year mark again, except that it establishes 50-year review for sensitive intelligence and cryptographic information. In addition, it requires the Archivist to establish priorities based upon the expected degree of researcher interest and the likelihood that review will result in significant declassification. While other agencies are not required to conduct systematic review for declassification of records in their custody, they are encouraged to do so if resources are available.

There is at least one area of the revised systematic review program that requires special scrutiny. By reducing and slowing down the program, E.O. 12356 potentially worsens a problem that has existed for some time, i.e., the buildup of permanently valuable classified records. This is especially true at a time when the National Archives has had to cut back on the resources it devotes to systematic review. A very positive program to counter this problem is the transfer of funds from a classifying agency to the National Archives so that it may systematically review specified records of that agency at a cost far less than would otherwise be the case. The State Department and the National Archives currently participate quite successfully in such a project. The agencies and ISOO must also pay particular attention to other variables that may counteract the buildup of classified holdings. These include educating original classifiers with respect to determining the duration of classification based upon specific dates or events, and discouraging the use of the waiver authority vested in agency heads with respect to both portion marking and the issuance of classification guides. Both portion marking and classification guides tend to control the volume of classified information, especially that classified on a derivative basis.

On balance, E.O. 12356's systematic review program represents a reasonable compromise between the calls to abolish the program and the costly, inefficient system under E.O. 12065. When properly administered and funded, systematic review remains the most effective means of declassifying large quantities of those classified records in the National Archives that are in greatest demand by researchers.

ADMINISTRATIVE REQUIREMENTS

When the Interagency Information Security Committee met on June 19, 1980, to consider the draft GAO report on systematic review, the discussion turned to other provisions of E.O. 12065 that the representatives of the member agencies felt were unworkable or inadvisable. Most of their other complaints expressed that day could be grouped under the heading, "Administrative Headaches."

In drafting E.O. 12065, its authors designed stringent administrative controls as a means to restrain unwarranted classification. These controls sought to limit classification authority initially; to inhibit the delegation of classification authority; to minimize the extension of automatic declassification dates; to mandate portion marking; to require the promulgation of classification guides; to restrict the classification of information following the receipt of a Freedom of Information or mandatory review request; and to ban the reclassification of any information that had previously been declassified and disclosed.

By and large most of these measures had the desired effect and E.O. 12356 retains their positive features. In some situations, however, the degree of inflexibility drafted into these provisions created unnecessary and unreasonable impediments to an effective information security system. Notable among these were the provision limiting agency classification action to the agency head or deputy agency head following the receipt of a Freedom of Information or mandatory review request; the universal requirement for classification guides; the requirement that only an agency head or "Top Secret" classification authority could issue a classification guide; and the total ban on reclassification.

Section 1-606 of E.O. 12065 provided in pertinent part: "No document . . . may be classified after an agency has received a request for the document under the Freedom of Information Act or the Mandatory Review provisions of this Order . . . unless such classification . . . is authorized by the agency head or deputy agency head." The rationale for this limitation is laudable, and carries over into E.O. 12356. It seeks to prevent agencies from unjustifiably using the classification system to thwart the general policy expressed by the Freedom of Information Act and mandatory review. Inherent in the provision is the assumption that limiting classification action under these circumstances to the agency head or deputy agency head helps assure its legitimacy.

Unfortunately, there are several government agencies that receive numerous Freedom of Information and mandatory review requests for large quantities of older records, which, although safeguarded from disclosure, have never been previously marked as national security information. Faced with requests for access to thousands upon thousands of these documents, many of them clearly and routinely classifiable, the requirement that only the agency head or deputy agency head could classify them became an enormous burden on their valuable and limited time. E.O. 12356 rectifies this situation by adding the "senior agency official," designated by the agency head, and agency "Top Secret" original classifiers, of whom there are less than 1,500 government-wide, as persons who may also classify information following the receipt of a Freedom of Information or mandatory review request. Because these individuals are by and large the same officials and policymakers who would be recommending classification to the agency heads, it is reasonable to expect that they will classify information with the discretion and judgment that these special circumstances demand.

The provision of E.O. 12065 mandating the development and issuance of classification guides also created administrative problems in certain agencies. A classification guide is a document issued by an original classification authority that instructs derivative classifiers about the particular elements of information that must be classified, the level of classification and its duration. In most instances guides help assure uniform classification and otherwise facilitate the derivative classification process. In some areas, however, it is difficult and sometimes impossible to predetermine and describe particular elements of information that must be classified. This has proven to be especially true in the area of foreign relations. As a result, in some cases the cost of producing usable guides far exceeds their benefits in facilitating derivative classification. Therefore, E.O. 12356 permits an agency head to waive the requirement to produce classification guides when an evaluation of relevant factors spelled out in ISOO Directive No. 1 reveals that the cost of production would exceed the benefit to the derivative classification process. The agency head must report waivers to the Director of ISOO, who will review them as part of the oversight function.

Ironically, another provision of E.O. 12065 hindered the promulgation of classification guides by limiting the authority to issue them to agency heads or original "Top Secret" classification authorities (only the agency head in those agencies that may not classify originally at the "Top Secret" level). In many instances the program official most familiar with the subject matter of a particular guide is an authorized original classifier, but not at the "Top Secret" level. Therefore, E.O. 12356 facilitates the promulgation of classification guides by permitting their issuance by an official who has program or supervisory responsibility over the information and is authorized to classify information originally at the highest level of classification prescribed in the guide.

Another area of inflexible administration was E.O. 12065's blanket prohibition against the reclassification of information previously declassified and disclosed. Almost anyone would agree that in most instances it is useless and sometimes counterproductive to reclassify information once it has been declassified and disclosed. However, there are exceptions. During the time E.O. 12065 was in effect, situations arose in which information had been declassified erroneously and disclosed, but the information was reasonably recoverable from the recipient. Despite the fact that the damage to the national security could be minimized, the blanket prohibition prevented reclassification. Rather than closing the door to reclassification completely, E.O. 12356 provides that information previously declassified and disclosed, but which continues to meet the tests for classification, may be reclassified by an agency head if it is "reasonably recoverable." ISOO Directive No. 1 specifies those factors that an agency head must take into consideration before reclassifying information under this provision. In addition, each reclassification action must be reported to the Director of ISOO, who closely monitors its reasonableness. These special safeguards should help assure that this authority is not abused.

A MATTER OF TONE

The Intelligence Community played a significant role in the development of E.O. 12356. In fact, it was an interagency Intelligence Community committee that composed the first draft of a revised Order. The committee acted in response to a White House request that it examine ways of improving the nation's intelligence capabilities. The committee focused its efforts on the negative tone of E.O. 12065 and those provisions of the Order that adversely impacted upon the Government's litigating posture in defending Freedom of Information and other lawsuits.

The problem of E.O. 12065's negative tone refers to its unbalanced portrayal of the twin goals of openness and security. The exhortation to openness that permeated its language distorted the fundamental purpose of an information security system, i.e., the protection of national security information from unauthorized disclosure. By repeatedly expressing the classification process in terms of "don'ts" rather than "dos," E.O. 12065 downplayed the critical importance of protecting our own sensitive information and the information given to the United States in confidence by foreign governments.

Given the tone of E.O. 12065's language, it is not surprising that foreign officials often expressed concern over the ability of this Government to protect shared information. They viewed the Order as an extension of the Freedom of Information Act. While these fears were largely unwarranted, this perception threatened to dry up actual and potential intelligence sources. The threat to the United States intelligence effort highlighted the need to state fundamental classification policy and procedures in language that recognized legitimate security requirements.

For example, Section 1-301 of E.O. 12065, which listed appropriate classification categories, began, "Information may not be considered for classification unless it concerns . . .." Contrast Section 1.3(a) of E.O. 12356: "Information shall be considered for classification if it concerns . . .." Similarly, Section 1-302 of E.O. 12065, which establishes the threshold damage test for classification, stated:

> Even though information is determined to concern one or more of the criteria in Section 1-301, it may not be classified unless an original classification authority also determines that its unauthorized disclosure reasonably could be expected to cause at least identifiable damage to the national security.

Contrast the positive statement of its revised counterpart, Section 1.3(b) of E.O. 12356:

> Information that is determined to concern one or more of the categories in Section 1.3(a) shall be classified when an original classification authority also determines that its unauthorized disclosure, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security.

Perhaps the clearest example of E.O. 12065's negative tone was found in the so-called "reasonable doubt" standard. This is the provision that instructs original classifiers if they are uncertain about the need to classify information, or about the appropriate classification level. Ironically, these respective provisions, which the news media and others have repeatedly and inaccurately cited to distinguish the two Orders in an extraordinarily abbreviated fashion, are far more important in theory than in practice. For even though the original classification process sometimes involves difficult judgments, the senior status of original classifiers encompasses officials who routinely make difficult decisions in areas related to national security. Accordingly, actual cases of "reasonable doubt" are unusual.

E.O. 12065 required that all these cases be resolved in favor of no classification, when whether to classify or not was the issue, and in favor of the lower classification level, when the appropriate level was the issue. This is a simplistic and dangerous solution. Why mandate an answer for all cases when the merits of each situation will differ and there exist reasonable means of resolution? E.O. 12356 takes a more responsible stance, providing, in effect, "When in doubt, find out." It requires that the information be safeguarded as if it were classified, or at the higher level, pending a determination by an authorized classifier, which must be reached within thirty days. This is certainly a reasonable delay when matters of national security are concerned.

With these and other changes in tone, E.O. 12356 sounds like what it is, the framework for the executive branch's information security system. While recognizing the critical importance of openness in government generally, it does not apologize for those situations in which the national security requires secrecy.

THE IMPACT OF LITIGATION

Several agencies frequently must defend in court their efforts to protect national security information from disclosure under the Freedom of Information Act. Executive Order 12065 unintentionally but significantly increased the burden upon the Government in defending these actions.

Section 3-303 of E.O. 12065 provided: "It is presumed that information which continues to meet the classification requirements [of the Order] requires continued protection. In some cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. . . ." This was the so-called "balancing test" of E.O. 12065.

For many months the drafters of E.O. 12065 debated the inclusion of a "balancing test." Proponents insisted that it was necessary to state explicitly that even properly classified records might be declassified for some greater public purpose than that served by their protection. Opponents, while recognizing the inherent need to balance the competing interests of protection and disclosure, warned against an explicit "balancing test" on the basis that it would create significant problems for the Government in defending Freedom of Information litigation. Ultimately, the proponents of a "balancing test" prevailed, on the assurance that the discretionary language quoted above would prevent its exploitation by plaintiffs in these lawsuits.

This forecast proved to be unequivocally wrong. The "balancing test" became, and in some holdover cases continues to be, the major litigating problem for the Government in actions involving E.O. 12065. Plaintiffs argued that the consideration of the "balancing test" by agency heads was mandatory, not discretionary, and challenged administrative determinations to keep information classified even when agency heads had applied the test. To defend these actions required the Government to prove not only the proper classification of information, but also the proper application of a "balancing" procedure. More ominous was the prospect that some judges would second-guess the agency heads, who were responsible under law for protecting the information, and who were knowledgeable about the consequences of disclosure. Finally, litigating the "balancing test" had the practical effect of requiring the defending agency to produce successive generations of supporting affidavits, increasing the details in each. This was not only burdensome, but it required the disclosure of more and more information about classified subjects, much of which was itself quite sensitive.

As in the case of the "balancing test," E.O. 12065's "identifiable" damage standard for "Confidential" classification is an example of good intentions leading to unexpected and undesirable consequences in the context of Freedom of Information litigation. The drafters of E.O. 12065 inserted the word "identifiable" to emphasize to classifiers the importance of conscious decision-making before classifying information. Instead, plaintiffs seized upon "identifiable" to argue that it mandated a qualitative or quantitative standard or degree of damage to national security before information could be classified. For example, in one lawsuit the plaintiff sought the release of certain information, which, if disclosed, would have revealed intelligence sources or methods. Plaintiff argued that it could not be classified, because the prospective damage to these sources or methods was merely speculative, and not presently "identifiable." Fortunately, the judge in this case recognized the absurdity of this logic. Nevertheless, the "identifiable" experience attests to the legal adage of avoiding unnecessary adjectives in drafting instruments subject to interpretation.

The drafters of E.O. 12356 agreed that the only realistic way to cope with these provisions adequately was to eliminate them. Less incisive action, e.g., alternative language, failed to exclude the possibility of persons continuing to litigate areas of administrative discretion.

The deletion of the "balancing test" should prove to be one of E.O. 12356's most important changes. Its absence should relieve much of the Government's unforeseen burden in defending Freedom of Information actions seeking access to classified records. ISOO and the classifying agencies must be vigilant, however, to see that the absence of the "balancing test" and "identifiable" damage does not result in less thoughtful classification and declassification decisions. Classifiers and declassifiers must consider both sides of the issue. As with prior Executive orders, E.O. 12356 does not require the classifier to record contemporaneously the reasons behind the decision to classify or to keep information classified. Every classifier must be aware, however, that there are avenues to challenge the validity of classification, at which time the classifier is likely to be called upon to justify and explain the classification decision in writing, and frequently under oath.

AUTOMATIC DECLASSIFICATION

Executive Orders 10501, 11652, and 12065 all included some provision for the automatic declassification of national security information based solely upon the passage of a fixed number of years. E.O. 12065 carried the concept of automatic declassification farthest:

> Section 1-401. Except as permitted in Section 1-402, at the time of the original classification each classification authority shall set a date or event for automatic declassification no more than six years later.
>
> Section 1-402. Only officials with Top Secret classification authority and agency heads . . . may classify information for more than six years from the date of original classification. This authority shall be used sparingly. . . .

What sounds good in theory doesn't always work. As happened with prior Orders, classifiers honored the automatic declassification requirements of E.O. 12065 far more frequently in the breach than in the practice. They could not ignore a reality that confronts classifiers much of the time: It is difficult, if not impossible, to discern at the time of classification the duration of the information's sensitivity.

In theory, uncertain classifiers under E.O. 12065 had two alternatives: (a) they could disregard their concern about the duration of the information's sensitivity, and mark the information for automatic declassification in six years or less; or (b) they could bring the information before the head of the agency or a "Top Secret" classification authority, and seek to have that person classify it for a period of time not to exceed twenty years (for foreign government information, not to exceed thirty years). In practice, classifiers chose alternative (a) less than 10 percent of the time. They chose alternative (b), requiring special procedures and mandated for "sparing" use, approximately 65 percent of the time.

In practice, to handle the remaining 25-30 percent of original classification actions, the classifiers relied upon an invention that wasn't even contemplated in E.O. 12065, i.e., "Review in six years." In other words, the classifiers, unwilling to risk the automatic declassification of information that might continue to require protection after six years, but also unwilling or unable to go through the procedure to extend its classification up to twenty years, created a makeshift substitute for automatic declassification.

Even though "six year review" may have eased the consciences of classifiers, it was not a viable solution. First, agencies were already having a difficult time trying to comply with the requirement to review 20-year old permanently valuable classified information. It was ludicrous to expect that they would be able to devote the resources necessary to review a large portion of all their classified information within six years. Second, because E.O. 12065 did not contemplate a "six-year review," it was quite possible that the courts would find that information marked in this manner was automatically declassified after six years, and order its release despite its national security sensitivity.

Information properly marked for six-year automatic declassification presented a different problem. ISOO and agency reviewers uncovered a disturbing number of situations in which the automatic declassification provisions of E.O. 12065 led to the rote application of the six-year rule to information that would clearly require protection for a longer period. This phenomenon was not new with E.O. 12065, merely exaggerated. Any classification system that mandates an arbitrary period of time for the duration of protection must presuppose some degree of premature disclosure and consequential damage to the national security.

E.O. 12065's system for automatic declassification was clearly one of its greatest failings. Over 90 percent of reported classification decisions fell outside its prescribed timeframe, and too many of the remaining decisions threatened the disclosure of information that continued to require national security protection. It was a situation serious enough to demand a fresh look at the concept of automatic declassification. Taking the bold step of bucking the trend of prior Orders, the drafters of E.O. 12356 concluded that the only rational approach was to abandon the myth of automatic declassification tied to a fixed period of years that may or may not have any relationship to the information's national security sensitivity. Instead, E.O. 12356 takes the only realistic approach, establishing the duration of classification for "as long as required by national security considerations." When they are able to do so, original classifiers are to establish specific dates or events for declassification at the time of classification. Otherwise, declassification follows an agency review, a process that may be initiated at any time by officials inside the agency, or citizens outside of it.

CONCLUSION

Executive Order 12356 is the product of a considerable effort to improve upon its moderately successful, if somewhat flawed, predecessor. Because it consolidates and expands upon the most successful features of prior information security systems, executive branch agencies have greeted its issuance enthusiastically.

At the same time, however, the traditional critics of the information security program have reacted, as could be predicted, negatively. At the heart of their criticism is the charge that the underlying purpose behind E.O. 12356 is to permit the classification of more information than could be classified under E.O. 12065. As this paper illustrates, the perceived flaws of E.O. 12065 did not include the breadth or scope of permissible classification. The authors of E.O. 12356 sought to provide better protection for that very small percentage of information that requires it, not to increase the amount or type of information to be classified.

Nevertheless, E.O. 12356 presents an important challenge to those who must implement it. Some of its critics will constantly scrutinize its implementation, hoping to uncover abuses that might be publicized to undermine its retention. Minimizing abuses represents the most effective countermeasure to this criticism. To do so, E.O. 12356's proponents must scrutinize its implementation even more thoroughly than its critics.